PRINTING CONTROLLER

Patent Number: JP11154070
Publication date: 1999-06-08
Inventor(s): ASANO SADAJI
Applicant(s): FUJI XEROX CO LTD
Requested Patent: ☐ JP11154070
Application Number: JP19970337674 19971121
Priority Number(s):
IPC Classification: G06F3/12; G06F13/00; G06F13/00
EC Classification:
Equivalents:

Abstract

PROBLEM TO BE SOLVED: To ensure security of printing data transfer, based upon the FTP protocol. SOLUTION: In a security user list 11, users who are allowed to perform security-printing are registered in advance. A user recognition part 10 stores received data in a security spool 90 on condition that a received user command as an FTP protocol command or information on a path command is registered in the list 11. A manual printing control part 13 reads a stored data out of the security spool 90 and transfers them to a printer engine when a security user name is inputted from a console 5 together with a printing request.

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平11－154070

(43)公開日　平成11年(1999)６月８日

(51)Int.Cl.[6]	識別記号	ＦＩ	
Ｇ０６Ｆ　3/12		Ｇ０６Ｆ　3/12	Ｄ
13/00	３５１	13/00	３５１Ｅ
	３５５		３５５

審査請求　未請求　請求項の数５　ＦＤ　（全６頁）

(21)出願番号　特願平9－337674

(22)出願日　平成９年(1997)11月21日

(71)出願人　000005496
富士ゼロックス株式会社
東京都港区赤坂二丁目17番22号

(72)発明者　浅野　貞二
埼玉県岩槻市府内３丁目７番１号　富士ゼロックス株式会社内

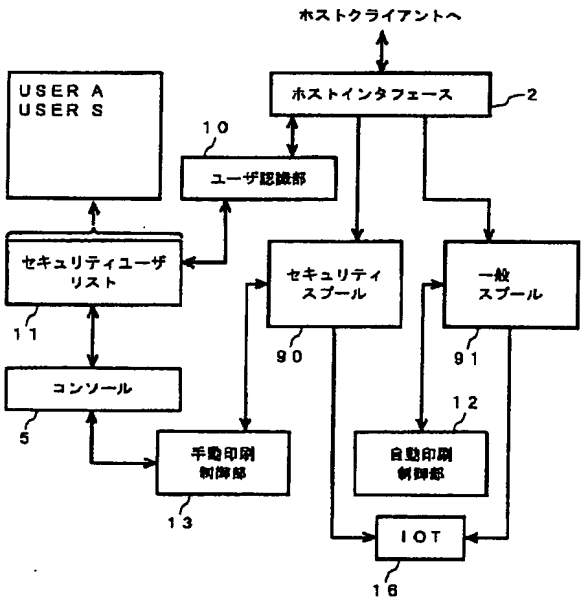
(74)代理人　弁理士　田中　香樹　(外１名)

(54)【発明の名称】　印刷制御装置

(57)【要約】

【課題】　ＦＴＰプロトコルを介した印刷データ転送のセキュリティを確保する。

【解決手段】　セキュリティユーザリスト１１には守秘印刷を許可されたユーザがあらかじめ登録される。ユーザ認識部１０は受信したＦＴＰプロトコルコマンドのユーザコマンドまたはパスコマンド上の情報がリスト１１に登録されている場合は、受信データをセキュリティスプール９０に格納する。手動印刷制御部１３は、コンソール５から印刷要求とともにセキュリティユーザ名が入力された場合に、格納されたデータをセキュリティスプールから読み出してプリンタエンジン１ｂに転送する。



1

【特許請求の範囲】

【請求項１】　ＦＴＰプロトコルを介して受信した印刷データを印刷するプリントサーバの印刷制御装置において、

セキュリティユーザ識別情報を登録したリストと、

受信した前記印刷データが守秘印刷ファイルであるか否かを、ＦＴＰプロトコルコマンド上のユーザ識別情報および前記リストに含まれているセキュリティユーザ識別情報を参照して判別する守秘印刷ファイル認識手段と、

前記守秘印刷ファイル認識手段によって守秘印刷ファイルであると判断された印刷データおよび前記ユーザ識別情報を格納する守秘印刷データ格納手段と、

セキュリティユーザ識別情報および印刷開始指示を入力する印刷開始指示手段と、

前記セキュリティユーザ情報および印刷開始指示の入力に応答して前記守秘印刷データ格納手段から印刷データを読み出す手動印刷制御手段と、

前記印刷データを印刷するプリンタエンジンとを具備したことを特徴とする印刷制御装置。

【請求項２】　前記印刷開始指示手段が、入力されたセキュリティユーザ情報が前記リストに登録されている場合に、前記手動印刷制御手段を有効にする許可信号を出力するように構成されていることを特徴とする請求項１記載の印刷制御装置。

【請求項３】　前記手動印刷制御手段が、前記許可信号を受けた後、さらに前記セキュリティユーザ情報および前記守秘印刷データ格納手段に格納されているユーザ識別情報の一致を条件として前記守秘印刷データ格納手段から印刷データを読み出すように構成されていることを特徴とする請求項２記載の印刷制御装置。

【請求項４】　前記リストに登録されているセキュリティユーザ情報は、守秘印刷ファイル転送を許可されたユーザの名称であって、

前記守秘印刷ファイル認識手段は、前記ＦＴＰプロトコルコマンドのユーザコマンドに含まれるユーザ名が前記リストのユーザ名称に含まれている場合に、受信した前記印刷データが守秘印刷ファイルであると判断するように構成されたことを特徴とする請求項１記載の印刷制御装置。

【請求項５】　前記リストに登録されているセキュリティユーザ情報は、守秘印刷ファイル転送を許可されたユーザにセキュリティ用として割り当てられたパスワードであって、

前記守秘印刷ファイル認識手段は、前記ＦＴＰプロトコルコマンドのパスコマンドに含まれるパスワードが前記リストのパスワードに含まれている場合に、受信した前記印刷データが守秘印刷ファイルであると判断するように構成されたことを特徴とする請求項１記載の印刷制御装置。

【発明の詳細な説明】

2

【０００１】

【発明の属する技術分野】本発明は、印刷制御装置に関し、特に、ネットワークを介して接続された印刷装置（以下、「プリンタ」という）で守秘印刷ファイルを印刷するのに好適な印刷制御装置に関する。

【０００２】

【従来の技術】ネットワークにコンピュータを接続したシステム形態として、汎用大型コンピュータつまりメインフレームを中心とした垂直型ネットワークが知られている。また、近年は、コンピュータ・システムのダウンサイジング（小型化）傾向により、ローカル・エリア・ネットワーク（ＬＡＮ）に複数のワークステーションを接続したシステム形態が増加している。

【０００３】このようなネットワーク環境下におかれたプリンタにおいて、機密保持を必要とするファイルつまり守秘印刷ファイルを印刷する場合がある。守秘印刷ファイルを安全に印刷するには、印刷要求者や予め守秘印刷ファイルを出力する資格を与えられているオペレータがプリンタのコンソール上で直接操作をして印刷を実行するのが最も望ましい。

【０００４】しかし、そのためには有資格者を、守秘印刷データの転送開始から印刷終了までプリンタに拘束する必要があり、実現が容易ではない。この問題点を解消するため、例えば、特開平７－１３４６８１号公報では、垂直型ネットワークにおける守秘印刷ファイルの印刷制御装置が開示されている。この印刷制御装置では、印刷データの転送時に該印刷データに付加されるジョブ情報を利用して、有資格者を拘束することなく守秘データの保護ができるようにしている。

【０００５】

【発明が解決しようとする課題】上記の印刷制御装置では、次のような問題点がある。水平型ネットワークに接続されるワークステーションやプリンタは、互いに共通する通信プロトコルを通じて会話やデータの授受をしている。

【０００６】水平型ネットワークで使用される通信プロトコルの種類は多く、ネットワーク上のワークステーションやプリンタがすべての通信プロトコルに対応することは困難である。そこで、現状のプリンタに最も一般的に実装されていると思われる標準的なファイル転送プロトコルであるＦＴＰプロトコルを少なくとも実装することにより、印刷データをファイルとしてプリンタに転送する方式をとることが多い。

【０００７】しかし、ＦＴＰプロトコルの規約上には守秘印刷ファイルの転送に関する規定はなく、セキュリティ確保の観点からは不十分であった。したがって、標準化されたファイル転送プロトコルであるＦＴＰプロトコルを変更することなく印刷ファイルから守秘印刷ファイルを識別してセキュリティを確保することができる方式が要望されていた。

3

【０００８】本発明は、上記問題点を解消し、汎用的なファイル転送プロトコルを変更することなく守秘印刷ファイルを区別することができる印刷制御装置を提供することを目的とする。

【０００９】

【課題を解決するための手段】上記の課題を解決し、目的を達成するための本発明は、ＦＴＰプロトコルを介して受信した印刷データを印刷するプリントサーバの印刷制御装置において、セキュリティユーザ識別情報を登録したリストと、受信した前記印刷データが守秘印刷ファイルであるか否かを、ＦＴＰプロトコルコマンド上のユーザ識別情報および前記リストに含まれているセキュリティユーザ識別情報を参照して判別する守秘印刷ファイル認識手段と、前記守秘印刷ファイル認識手段によって守秘印刷ファイルであると判断された印刷データおよび前記ユーザ識別情報を格納する守秘印刷データ格納手段と、セキュリティユーザ識別情報および印刷開始指示を入力する印刷開始指示手段と、前記セキュリティユーザ識別情報および印刷開始指示の入力に応答して前記守秘印刷データ格納手段から印刷データを読み出す手動印刷制御手段と、前記印刷データを印刷するプリンタエンジンとを具備した点に特徴がある。

【００１０】上記特徴によれば、ＦＴＰプロトコルコマンド上のユーザ識別情報が、予定のリスト上にあるか否かによって印刷データが守秘印刷ファイルであるか否かが判断され、その判断結果によって守秘印刷ファイルは守秘印刷データ格納手段に格納される。さらに、この守秘印刷ファイルはセキュリティユーザ識別情報が入力したときにプリンタエンジンに読み出される。

【００１１】

【発明の実施の形態】以下、本発明の実施形態を図面を参照して詳細に説明する。図２は、本発明の一実施例に係るプリント制御装置を含むプリントサーバの構成を示すブロック図である。同図において、プリントサーバ１はプリンタ制御装置１ａとプリンタエンジンつまりイメージ出力端末（ＩＯＴ）１ｂとからなる。プリンタ制御装置１ａはホストインタフェース（Ｉ／Ｆ）２を通じてクライアントホスト３から印刷データを受信する。受信された印刷データはラスタライズされた後、プリンタインタフェース（Ｉ／Ｆ）４を通じてＩＯＴ１ｂに転送されて印刷される。

【００１２】プリンタ制御装置１ａはキーボード等の入力手段およびディスプレイ装置を含む操作装置（コンソール）５と、ＲＯＭ６、ＲＡＭ７およびＣＰＵ８からなるマイクロコンピュータで実現できる。なお、補助記憶装置として固定ディスク装置９が設けられる。

【００１３】プリントサーバ１のホストインタフェース２およびクライアントホスト３はＦＴＰプロトコルを実行するプログラム、すなわちＦＴＰサーバプログラムおよびＦＴＰクライアントプログラムをそれぞれ実行する

4

機能を有している。

【００１４】図１は，前記プリントサーバ１の要部制御機能を示すブロック図である。ＦＴＰサーバプログラムを実行するホストインタフェース２はＦＴＰプロトコル処理を実行してクライアントホスト３から印刷データを受信する。ホストインタフェース２はＦＴＰのログイン要求時に、受信したＦＴＰコマンドのユーザコマンド(USER)のパラメータの一つとして記述されているユーザ名が有資格者名であるか否かを判別する。具体的には、守秘印刷ファイルを認識する手段としてのユーザ認識部１０において、前記ユーザコマンドとセキュリティユーザリスト１１に登録されているセキュリティユーザ情報としてのセキュリティユーザ名すなわち守秘印刷ファイルの印刷を許可されている有資格者名とを比較して識別する。セキュリティユーザ名はあらかじめコンソール５からオペレータによって入力されている。図示の例ではユーザＡとユーザＳとがセキュリティユーザとして登録されている。

【００１５】セキュリティスプール９０には、前記ユーザコマンドがセキュリティユーザリスト１１上のセキュリティユーザ名に含まれていた場合に、受信した印刷データが格納される。一方、一般スプール９１には、前記ユーザコマンドがセキュリティユーザリスト１１上のセキュリティユーザ名に含まれていなかった場合に、受信した印刷データが格納される。

【００１６】一般スプール９１に格納された印刷データは、ひとつのプリントジョブ分の印刷データがそろったときに自動印刷制御部１２によって順次ＩＯＴ１ｂに自動的に転送される。また、セキュリティスプール９０に格納された印刷データは、手動印刷制御部１３によってユーザ名の確認処理を経た後、ＩＯＴ１ｂに転送される。

【００１７】コンソール５は、ユーザ名が入力されると、そのユーザ名がセキュリティユーザリスト１１に登録されているかどうかを判別し、ユーザ名が登録されている場合に、手動印刷制御部１３を有効にする許可信号を出力する。手動印刷制御部１３は、コンソール５から前記許可信号を受信すると、その次にコンソール５から入力されるユーザ名を、セキュリティスプール９０に印刷データとともに格納されているユーザ名と比較する。比較の結果、両ユーザ名が一致していた場合に、セキュリティスプール９０から印刷データを読み出してＩＯＴ１ｂに転送する。

【００１８】上記プリンタ制御装置の処理をフローチャートを参照して説明する。図３においてステップＳ１では、ＦＴＰコマンドを受信したか否かを判断し、判断が肯定ならばステップＳ２に進み、ユーザコマンドがセキュリティユーザリスト１１に登録されているか否かを判断する。この判断が肯定ならばステップＳ３に進み、受信した印刷データをセキュリティスプール９０に格納す

る。ステップＳ２が否定ならばステップＳ４に進み、一般スプール９１に受信した印刷データを格納する。

【００１９】図４は印刷時のフローチャートである。ステップＳ１０では、印刷要求を待つ。コンソール５から印刷要求が入力されるとステップＳ１１に進む。ステップＳ１１では、ユーザ名の入力を促す表示をコンソール５の表示画面に出力する。ステップＳ１２では、入力されたユーザ名がセキュリティユーザリスト１１に登録されているか否かを判断する。この判断が肯定ならばステップＳ１３に進み、セキュリティスプール９０に受信した印刷データとともに格納されているユーザ名と、コンソール５から印刷要求とともに入力されたユーザ名とが一致しているか否かを判断する。

【００２０】ユーザ名が一致したならばステップＳ１４に進み、セキュリティスプール９０上の印刷データをＩＯＴ１ｂに転送する。ユーザ名が一致しない場合、またはユーザ名がセキュリティユーザリスト１１に登録されていない場合は、ステップＳ１２，Ｓ１３からステップＳ１５に移行する。ステップＳ１５では、例えば「印刷不可」の表示をコンソール５に出力するエラー処理をする。

【００２１】図５は、クライアントホスト３とプリントサーバ１との間でのＦＴＰプロトコルのコマンドシーケンスである。同図において、クライアントホスト３から接続要求が出されるとプリントサーバ１がこれに応答し、引き続いて、クライアントホスト３からユーザコマンド(USER)とパスコマンド(PASS)が送出され、プリントサーバから、これらのコマンドの応答があるとログイン成功が確認される。ログインが成功した後は、目的に応じて種々のコマンドシーケンスを取り得るが、ここでは、ファイル転送を目的とした簡単なシーケンスを一例としてあげている。

【００２２】ログイン成功の後、クライアントホスト３はタイプコマンド(TYPE)により、バイナリやＡＳＣＩＩといったファイルタイプを知らせる。ファイルタイプにより転送方式が異なるからである。さらに、クライアントホスト３は、ポートコマンド(PORT)により、ファイル転送に必要なポート番号をプリントサーバ１に通知する。最後に、クライアントホスト３はストアコマンド(STOR)を発行して、転送するファイル名とファイル転送要求をする。

【００２３】ストアコマンドを受けとったプリントサーバ１は先に受けとったポートコマンドのポート番号を用いてデータ転送用の新たなコネクションを開設する。クライアントホスト３はプリントサーバ１からストアコマンドに対する転送許可応答を受信後、プリントサーバ１に対するデータの転送を開始する。データの終了を示すコマンドＥＯＦをプリントサーバ１が受けとった後、プリントサーバ１からの終了確認応答をもってデータ転送は終了する。上述の実施形態では、上記ＦＴＰシーケンスで必ずクライアントホスト３から送出されるユーザコマンドのパラメータの一つとして設定されるユーザ名を判別してセキュリティ処理をした。

【００２４】続いて、本願発明の第２実施形態を説明する。この第２実施形態では、図５に示したシーケンスにおけるパスコマンド(PASS)のパラメータとして設定されたパスワードに基づいてセキュリティユーザの判別をする。したがって、前記セキュリティユーザリスト１１は図６のように変形する。図６において、セキュリティユーザリスト１１ではそれぞれのユーザ名には二つのパスワードが登録されている。第１のパスワード（パス１）は、一般ユーザのパスワードであり、第２のパスワード（パス２）は、セキュリティユーザのパスワードである。すなわち、二つのパスワードをもつことによって、例えばユーザＡは、一般ファイルを印刷したいときは、ユーザ名(USERA) とパス１(com) をパスコマンドに記述し、セキュリティファイルを印刷したいときには、ユーザ名(USERA) とパス２(SEC) をパスコマンドに記述するようにする。

【００２５】この第２実施形態においては、前記ユーザ認識部１０は、ユーザコマンドとパスコマンドとを受信した時点でパスコマンドに記述されているパスワードがセキュリティユーザリスト１１に登録されているパス１であれば、受信した印刷データを前記一般スプール９１に格納し、パスワードがパス２であれば、受信した印刷データをセキュリティスプール９０に格納する。

【００２６】また、セキュリティスプール９０に格納されている印刷データをＩＯＴ１ｂに出力する場合は、コンソール５から入力されたパスワードと図６のセキュリティユーザリスト１１のパスワード（パス２）とを比較した結果により手動印刷制御部１３を有効にする。そして、さらに、コンソール５から入力されたパスワードがセキュリティスプール９０に印刷データとともに格納されているパスワードと一致した場合に印刷データがセキュリティスプール９０からＩＯＴ１ｂに転送される。

【００２７】第２実施形態では、第１実施形態に関して説明したユーザ名の判別処理がパスワードの判別処理に置き換えられた点を除き、処理内要は図１～図４に示した例と同様である。このように第２実施形態では二つのパスワードのうちいずれがＦＴＰプロトコルコマンドに含まれているかを判断して一般印刷ファイルか守秘印刷ファイルかを区別した。したがって、ユーザは、いずれのパスワードを使用するかによって、自己の印刷要求対象であるファイルを一般スプールおよびセキュリティスプールのいずれか所望のものに格納することができる。

【００２８】

【発明の効果】以上の説明から明らかなように、本発明によれば、印刷データの転送に広く使用されているＦＴＰプロトコルコマンドを変更することなく、かつクライアントホスト側、つまり印刷データ供給側のＦＴＰプロ

グラムに変更を加えることなく守秘印刷ファイルのセキュリティを確保することができる。すなわち、クライアントホスト側では、プリントサーバ側のセキュリティ機能を意識することなく処理が可能であるため、既存のネットワーク上において容易にセキュリティシステムを実現することができる。

【図面の簡単な説明】

【図１】　本発明の一実施形態に係るプリントサーバの要部制御機能を示すブロック図である。

【図２】　本発明の一実施形態に係るプリントサーバの要部ハード構成を示すブロック図である。

【図３】　印刷データのスプール格納処理のフローチャートである。

【図４】　印刷印刷処理のフローチャートである。

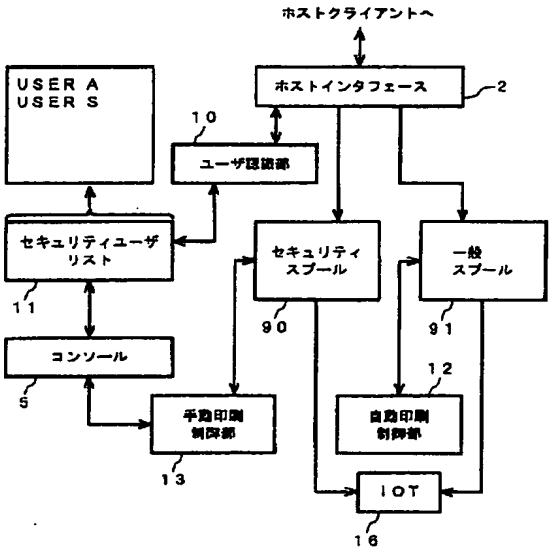
【図５】　ＦＴＰプロトコルのシーケンス図である。

【図６】　ユーザ識別情報を登録したリストの一例を示す図である。

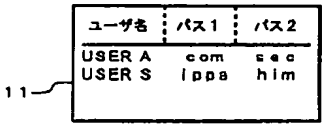
【符号の説明】

１…プリントサーバ、　１ａ…プリンタ制御装置、　１ｂ…プリンタエンジン、３…クライアントホスト、　５…コンソール、　１０…ユーザ認識部、　１１…セキュリティユーザリスト、　１３…手動印刷制御部、　９０…セキュリティスプール、　９１…一般スプール

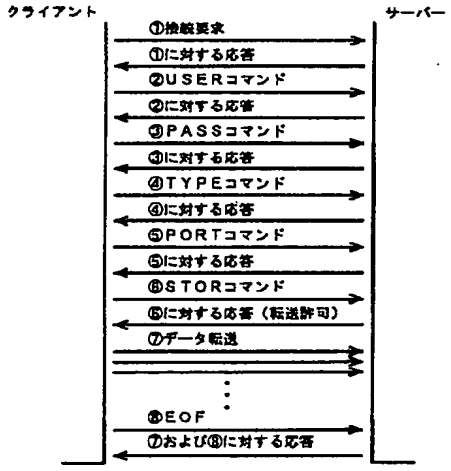
【図１】



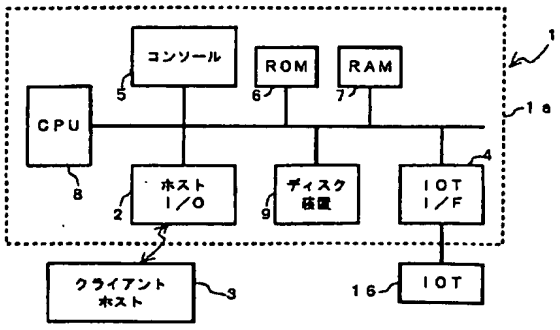
【図６】



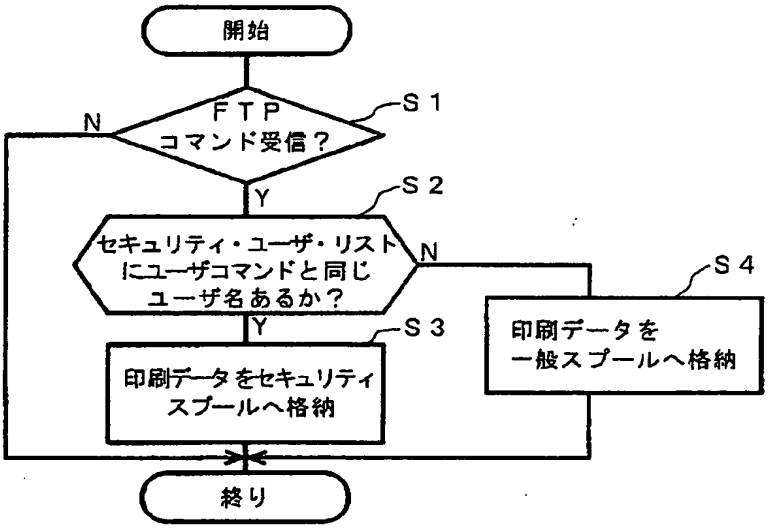
【図５】



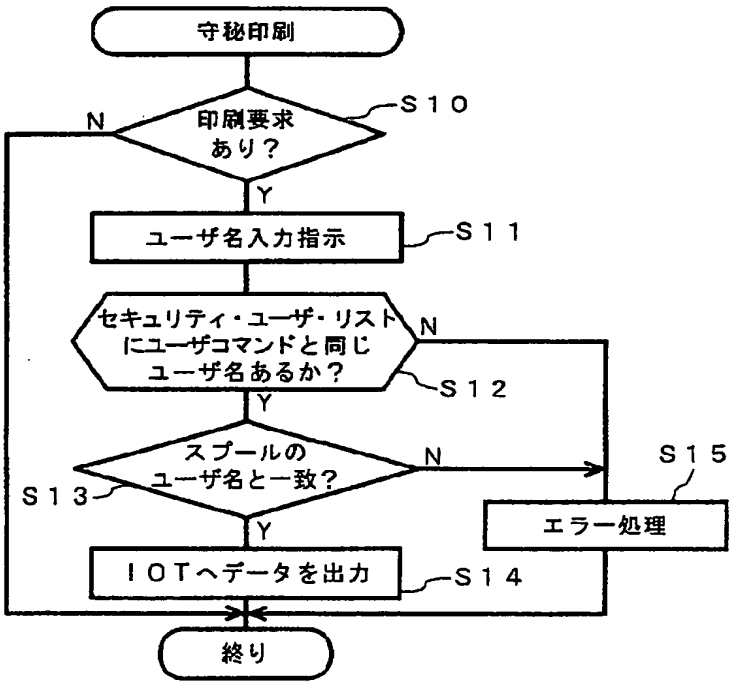
【図２】



【図３】


開始
ＦＴＰ
コマンド受信？
S１
N
Y
S２
セキュリティ・ユーザ・リスト
にユーザコマンドと同じ
ユーザ名あるか？
N
Y
S３
印刷データをセキュリティ
スプールへ格納
S４
印刷データを
一般スプールへ格納
終り

【図４】


守秘印刷
印刷要求
あり？
S１０
N
Y
ユーザ名入力指示
S１１
セキュリティ・ユーザ・リスト
にユーザコマンドと同じ
ユーザ名あるか？
N
S１２
Y
スプールの
ユーザ名と一致？
N
S１３
S１５
Y
エラー処理
ＩＯＴへデータを出力
S１４
終り

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-154070
(43)Date of publication of application : 08.06.1999

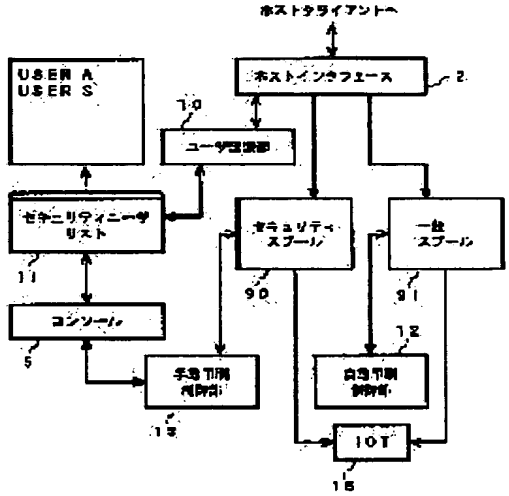
(51)Int.Cl. G06F 3/12
G06F 13/00
G06F 13/00

(21)Application number : 09-337674
(22)Date of filing : 21.11.1997

(71)Applicant : FUJI XEROX CO LTD
(72)Inventor : ASANO SADAJI

(54) PRINTING CONTROLLER

(57)Abstract:
PROBLEM TO BE SOLVED: To ensure security of printing data transfer, based upon the FTP protocol.
SOLUTION: In a security user list 11, users who are allowed to perform security-printing are registered in advance. A user recognition part 10 stores received data in a security spool 90 on condition that a received user command as an FTP protocol command or information on a path command is registered in the list 11. A manual printing control part 13 reads a stored data out of the security spool 90 and transfers them to a printer engine when a security user name is inputted from a console 5 together with a printing request.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

DETAILED DESCRIPTION

[Detailed Description of the Invention]
[0001]
[The technical field to which invention belongs] this invention relates to a suitable print control unit to print a **** print file by the printer (henceforth a "printer") especially connected through the network about a print control unit.
[0002]
[Description of the Prior Art] As a system gestalt which connected the computer to the network, the vertical-type network centering on a general-purpose large-sized computer, i.e., a mainframe, is known. Moreover, the system gestalt which connected two or more workstations to the local area network (LAN) is increasing in recent years according to the downsizing (miniaturization) inclination of computer system.
[0003] It may print in the printer set under such a network environment, the file, i.e., the **** print file, which needs a security protection. In order to print a **** print file safely, it is most desirable for the operator to whom a printing claimant and the qualification for outputting a **** print file beforehand are given to do a direct control on the console of a printer, and to perform printing.
[0004] However, it is necessary to restrain a qualified person to a printer from the transfer start of **** print data to a printing end, and, for that, realization is not easy. In order to cancel this trouble, in JP,7-134681,A, the print control unit of the **** print file in a vertical-type network is indicated. In this print control unit, it can be made to perform protection of **** data using the job information added to these print data at the time of a transfer of print data, without restraining a qualified person.
[0005]
[Problem(s) to be Solved by the Invention] There are the following troubles in the above-mentioned print control unit. The workstation connected to a level type network and the printer are carrying out conversation and transfer of data through the communications protocol which is mutually common.
[0006] There are many kinds of communications protocol used in a level type network, and it is difficult for the workstation and printer on a network to deal with all communications protocols. Then, the method transmitted to a printer by considering print data as a file is taken in many cases by mounting at least the FTP protocol which is a standard file transfer protocol considered to be mounted to the present printer most generally.
[0007] However, there was no convention about a transfer of a **** print file on the agreement of a FTP protocol, and it was inadequate for it from a viewpoint of security reservation. Therefore, the method which can discriminate a **** print file from a print file, and can secure security was demanded, without changing the FTP protocol which is a standardized file transfer protocol.
[0008] this invention cancels the above-mentioned trouble, and it aims at offering the print control unit which can distinguish a **** print file, without changing a general-purpose file transfer protocol.
[0009]
[Means for Solving the Problem] this invention for solving the above-mentioned technical problem and attaining the purpose In the print control unit of the print server which prints the print data which received through the FTP protocol Whether the aforementioned print data which received are **** print files [the list which registered security user-identification information, and] A **** print file recognition means to distinguish with reference to the security user-identification information included in the user-identification information on a FTP protocol command, and the aforementioned list, A **** print-data storing means to store the print data and the aforementioned user-identification information which were judged to be a **** print file by the aforementioned **** print file recognition means, A printing start directions means to input security user-identification information and printing start directions, The feature is in the point of having provided the manual printing control means which answer the input of the aforementioned security user-identification information and printing start directions, and read print data from the aforementioned ****

print-data storing means, and the printer engine which prints the aforementioned print data.
[0010] According to the above-mentioned feature, it is judged by whether the user-identification information on a FTP protocol command is on the list of schedules whether print data are **** print files, and a **** print file is stored in a **** print-data storing means by the judgment result. Furthermore, this **** print file is read to a printer engine, when security user-identification information inputs.
[0011]
[Embodiments of the Invention] Hereafter, the operation gestalt of this invention is explained in detail with reference to a drawing. Drawing 2 is the block diagram showing the composition of the print server containing the print control unit concerning one example of this invention. A print server 1 consists of printer control unit 1a and printer engine (IOT), i.e., end of image outgoing end, 1b in this drawing. Printer control unit 1a receives print data from the client host 3 through a host interface (I/F) 2. After being rasterized, through a printer interface (I/F) 4, the received print data are transmitted to IOT1b, and are printed.
[0012] Printer control unit 1a is realizable with the microcomputer which serves as the operating set (console) 5 containing an input means and display units, such as a keyboard, from ROM6, RAM7, and CPU8. In addition, fixed-disk equipment 9 is formed as auxiliary memory.
[0013] The host interface 2 and the client host 3 of a print server 1 have the function to perform the program which performs a FTP protocol, i.e., a FTP server program, and a FTP client program, respectively.
[0014] Drawing 1 is the block diagram showing the important section control function of the aforementioned print server 1. The host interface 2 which performs a FTP server program performs FTP protocol processing, and receives print data from the client host 3. The user name described as one of the parameters of the user command (USER) of the FTP command which the host interface 2 received to the login demand of FTP distinguishes whether it is a qualified person name. The qualified person name to which printing of the security user name as security user information registered into the aforementioned user command and the security user list 11, i.e., a **** print file, is specifically permitted in the user recognition section 10 as a means which recognizes a **** print file is compared and discriminated. The security user name is beforehand inputted by the operator from the console 5. In the example of illustration, User A and User S are registered as a security user.
[0015] When the aforementioned user command is contained in the security user name on the security user list 11, the print data which received are stored in the security spool 90. On the other hand, when the aforementioned user command is not contained in the security user name on the security user list 11, the print data which received are stored in the common spool 91.
[0016] The print data stored in the common spool 91 are automatically transmitted one by one to IOT1b by the automatic printing control section 12, when the print data for one print SHOBU gather. Moreover, after the print data stored in the security spool 90 pass through check processing of a user name by the manual printing control section 13, they are transmitted to IOT1b.
[0017] A console 5 outputs the enabling signal which confirms the manual printing control section 13, when it distinguishes whether the user name is registered into the security user list 11 and the user name is registered, if a user name is inputted. The manual printing control section 13 compares the user name inputted into the degree from a console 5 with the user name in which it is stored by the security spool 90 with print data, if the aforementioned enabling signal is received from a console 5. When both user names are in agreement as a result of comparison, print data are read from the security spool 90, and it transmits to IOT1b.
[0018] Processing of the above-mentioned printer control unit is explained with reference to a flow chart. If it judges whether the FTP command was received at Step S1 and judgment is affirmation in drawing 3 , it will progress to Step S2, and it judges whether the user command is registered into the security user list 11. If this judgment is affirmation, the print data which progressed to Step S3 and received are stored in the security spool 90. If Step S2 is negative, it will progress to Step S4, and the print data which received to the common spool 91 are stored.
[0019] Drawing 4 is a flow chart at the time of printing. It waits for a printing demand at Step S10. If a printing demand is inputted from a console 5, it will progress to Step S11. At Step S11, the display to which the input of a user name is urged is outputted to the display screen of a console 5. At Step S12, it judges whether the inputted user name is registered into the security user list 11. If this judgment is affirmation, it will progress to Step S13, and it judges whether the user name stored with the print data which received to the security spool 90, and the user name inputted with the printing demand from the console 5 are in agreement.
[0020] If a user name is in agreement, it will progress to Step S14, and the print data on the security spool 90 are transmitted to IOT1b. When a user name is not in agreement, or when the user name is not registered into the security user list 11, it shifts to Step S15 from Steps S12 and S13. At Step S15, error processing which outputs the display with "improper" printing to a console 5, for example is carried out.

[0021] Drawing 5 is the command sequence of the FTP protocol between the client host 3 and a print server 1. In this drawing, succeedingly, if a connection request is advanced from the client host 3, a print server 1 will answer this, and a user command (USER) and a path command (PASS) are sent out from the client host 3, and from a print server, if there is a response of these commands, a login success will be checked. Although various command sequences can be taken according to the purpose after login is successful, the easy sequence aiming at a file transfer is raised as an example here.

[0022] The client host 3 tells file types, such as a binary and ASCII, with a type command (TYPE) after a login success. It is because the transmittal mode changes with file types. Furthermore, the client host 3 notifies a port number required for a file transfer to a print server 1 with a port command (PORT). Finally, the client host 3 publishes a store command (STOR), and gives a file transfer demand to the file name to transmit.

[0023] The print server 1 which received the store command establishes the new connection for data transfer using the port number of the port command received previously. The client host 3 starts the data transfer to a print server 1 after receiving the transfer permission response to a store command from a print server 1. After a print server 1 receives the command EOF which shows the end of data, data transfer is ended with the end Acknowledgement from a print server 1. With the above-mentioned operation form, the user name set up as one of the parameters of the user command surely sent out from the client host 3 by the above-mentioned FTP sequence was distinguished, and security processing was carried out.

[0024] Then, the 2nd operation gestalt of the invention in this application is explained. With this 2nd operation gestalt, a security user is distinguished based on the password set up as a parameter of the path command (PASS) in the sequence shown in drawing 5 . Therefore, the aforementioned security user list 11 is transformed like drawing 6 . In drawing 6 , two passwords are registered into each user name by the security user list 11. The 1st password (path 1) is a general user's password, and the 2nd password (path 2) is a security user's password. That is, when for example, the user A wants to print a general file by having two passwords, it is a user name (USERA). Path 1 (com) When you want to describe to a path command and to print a security file, it is a user name (USERA). Path 2 (SEC) It is made to describe to a path command.

[0025] When the aforementioned user recognition section 10 receives a user command and a path command in this 2nd operation gestalt, the print data which received when the password described by the path command was the path 1 registered into the security user list 11 are stored in the aforementioned general spool 91, and if a password is a path 2, the print data which received are stored in the security spool 90.

[0026] Moreover, when outputting the print data stored in the security spool 90 to IOT1b, the manual printing control section 13 is confirmed by the result which compared with the password (path 2) of the security user list 11 of drawing 6 the password inputted from the console 5. And when in agreement with the password with which the password inputted from the console 5 is further stored in the security spool 90 with print data, print data are transmitted to IOT1b from the security spool 90.

[0027] It is the same as that of the example shown in drawing 1 - drawing 4 in short in processing except for the point that distinction processing of the user name explained about the 1st operation gestalt was transposed to distinction processing of a password with the 2nd operation gestalt. In this way, with the 2nd operation gestalt, it judged any are contained in the FTP protocol command among two passwords, and the general print file or the **** print file was distinguished. Therefore, a user can store in any of a common spool and a security spool, or a desired thing the file which is the candidate for a printing demand of self by whether which password is used.

[0028]

[Effect of the Invention] The security of a **** print file can be secured without [without it changes the FTP protocol command currently widely used for the transfer of print data according to this invention so that clearly from the above explanation, and] adding change to the FTP program by the side of a client host, i.e., print-data supply. That is, in a client host side, without being conscious of the security function by the side of a print server, since it can process, a security system can be easily realized on the existing network.

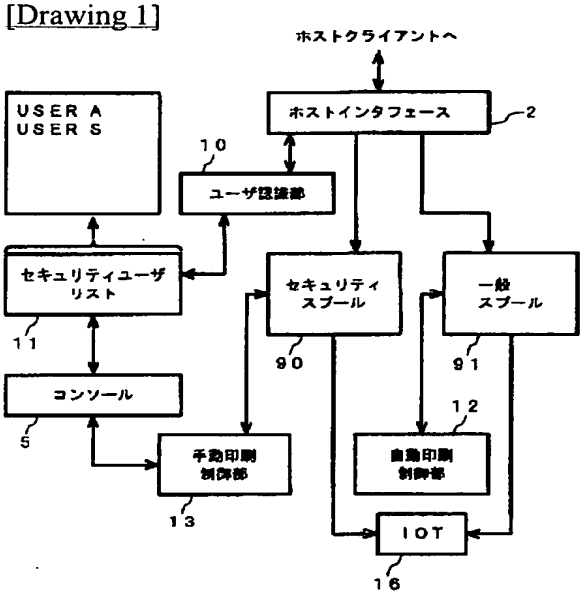
[Translation done.]

* NOTICES *

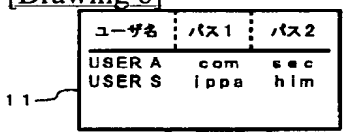
1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

DRAWINGS

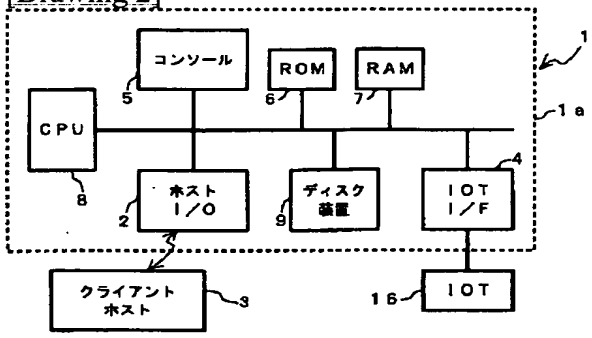
[Drawing 1]



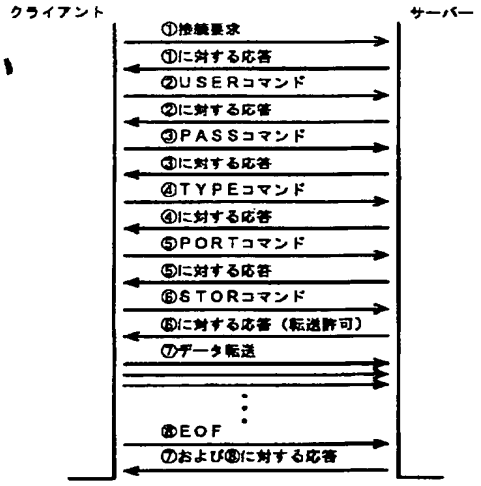
[Drawing 6]



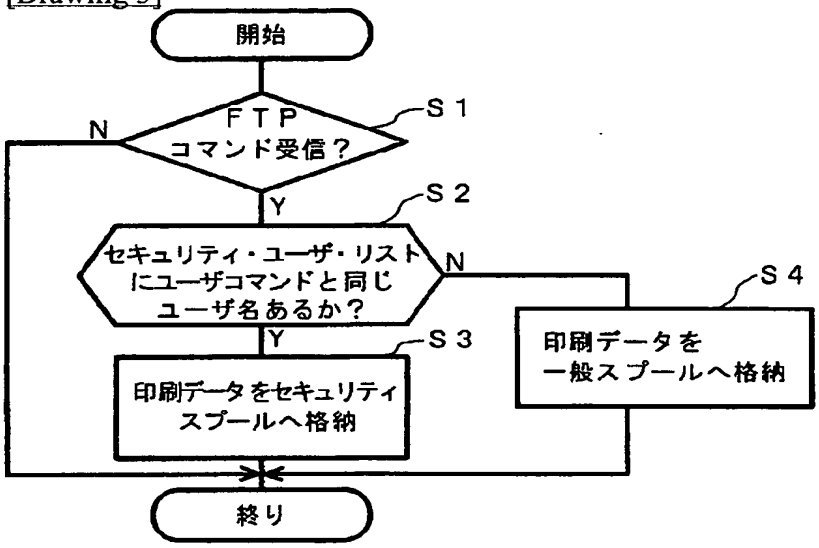
[Drawing 2]



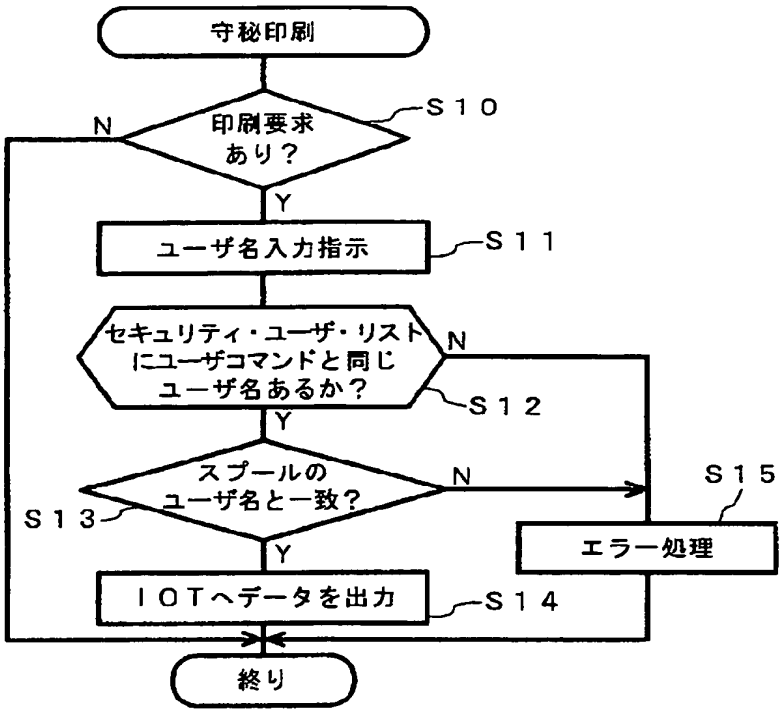
[Drawing 5]



[Drawing 3]



[Drawing 4]



[Translation done.]